PATENT ABSTRACTS OF JAPAN

(11)Publication number : 01-217689
(43)Date of publication of application : 31.08.1989

(51)Int.Cl. G06K 19/00
B42D 15/02

(21)Application number : 63-043461
(22)Date of filing : 26.02.1988

(71)Applicant : TOSHIBA CORP
(72)Inventor : IIJIMA YASUO

(54) PORTABLE ELECTRONIC EQUIPMENT

(57)Abstract:
PURPOSE: To diversify a method for establishing the security of an IC card system by registering plural cumulative upper limit values referred at the time of the discord of the collation of a password number and selecting the cumulative upper limit based on a corresponding relation determined in the IC card.
CONSTITUTION: The plural cumulative upper limit values referred at the time of the discord of the collation of the password number are registered, for instance, to select the cumulative upper limit value based on the corresponding relation determined in a main device. Accordingly, the referred cumulative upper limit values are not commonly used to the plural password numbers to establish the difference of the security level of the password number itself. Thereby, the method for establishing the security of the IC card system can be diversified.

LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

⑲日本国特許庁(JP)　⑪特許出願公開

⑫公開特許公報(A)　平1-217689

⑤Int.Cl.⁴	識別記号	庁内整理番号	㊸公開　平成1年(1989)8月31日
G 06 K 19/00		P-6711-5B	
B 42 D 15/02	331	J-8302-2C	
G 06 K 19/00		R-6711-5B	審査請求　未請求　請求項の数 1　(全11頁)

㊹発明の名称　携帯可能電子装置

㉑特　願　昭63-43461
㉒出　願　昭63(1988)2月26日

㉗発明者　飯島　康雄　神奈川県川崎市幸区柳町70番地　株式会社東芝柳町工場内
㉑出願人　株式会社東芝　神奈川県川崎市幸区堀川町72番地
㉔代理人　弁理士　鈴江　武彦　外2名

明　細　書

1．発明の名称

携帯可能電子装置

2．特許請求の範囲

メモリ部と、このメモリ部に対してデータの読出しおよび書込みを行なうための制御部を有し、選択的に外部からの入出力を行なう手段を具備する携帯可能電子装置であって、

前記メモリ部に記憶されている複数の第1のデータ列と、

外部から入力された第2のデータ列と前記メモリ部に記憶されている前記複数の第1のデータ列のうち選択的に1つの第1のデータ列とを両者の間に所定の関係があるか否か照合する照合手段と、

この照合手段の照合結果が否定的であった際その否定回数を累積する累積手段と、

複数の累積上限値を記憶する記憶手段と、

この記憶手段から前記累積手段で累積された回数と比較するための1つの累積上限値を選択する選択手段と、

この選択手段で選択された累積上限値と前記累積手段で累積された回数とを比較する比較手段と、

この比較手段の比較結果に基づき前記複数の第1のデータ列のうち選択された第1のデータ列の使用を禁止する禁止手段と

を具備したことを特徴とする携帯可能電子装置。

3．発明の詳細な説明

〔発明の目的〕

(産業上の利用分野)

本発明は、たとえばクレジットカードやキャッシュカードなどとして用いられる、いわゆるICカードと称される携帯可能電子装置に関する。

(従来の技術)

近年、クレジットカードやキャッシュカードなどの磁気ストライプ付カード、いわゆる磁気カードが普及している中、これらに代わって新たに記憶容量を拡大した、消去可能な不揮発性メモリおよび、これらを制御するCPUなどの制御素子を有するICチップを内蔵した、いわゆるICカードが注目されている。

このようなＩＣカードが運用されるシステムとして、最近では複数のアプリケーションを１つのＩＣカードで利用する動きがある。ＩＣカードの利用時には、本人確認を行なうために暗証番号の照合を行なうようになっている。

すなわち、あらかじめＩＣカードのメモリ内に暗証番号を登録しておき、外部装置にて暗証番号を入力することにより、この入力された暗証番号と登録された暗証番号との照合をカード内部で行なう。そして、この照合結果に基づき、以降のオペレーションの可否をカード自身で判断することにより、メモリ内のデータのセキュリティ保持を実現している。また、照合不一致の際には、不一致回数をカード内で累積し、あらかじめメモリ内に登録されている累積上限値（リミット値）との比較を行ない、累積回数がその累積上限値に達すると、以降その暗証番号が使用不可能となるよう制御している。

さて、先に述べたようにシステムが複雑化するにつれ、ＩＣカードに登録される暗証番号の数も多くなり、その運用セキュリティレベルもそれぞれ異なる。しかるに、累積上限値が複数の暗証番号の全てに対して共通に用いられると、この運用セキュリティレベルの差が実現しにくくなる。

（発明が解決しようとする課題）

本発明は、上記したように暗証番号の照合不一致時に参照する累積上限値が複数の暗証番号に対して共通に使用されると、暗証番号自身のセキュリティレベルの格差を確立できなくなるという問題点を解決すべくなされたもので、暗証番号の照合不一致時に参照する累積上限値が複数の暗証番号に対して共通に使用されなくなり、暗証番号自身のセキュリティレベルの格差を確立できる携帯可能電子装置を提供することを目的とする。

［発明の構成］

（課題を解決するための手段）

本発明は、メモリ部と、このメモリ部に対してデータの読出しおよび書込みを行なうための制御部を有し、選択的に外部からの入出力を行なう手段を具備する携帯可能電子装置であって、前記メモリ部に記憶されている複数の第１のデータ列（たとえば暗証番号）と、外部から入力された第２のデータ列（たとえば暗証番号）と前記メモリ部に記憶されている前記複数の第１のデータ列のうち選択的に１つの第１のデータ列とを両者の間に所定の関係があるか否か照合する照合手段と、この照合手段の照合結果が否定的であった際その否定回数を累積する累積手段と、複数の累積上限値を記憶する記憶手段と、この記憶手段から前記累積手段で累積された回数と比較するための１つの累積上限値を選択する選択手段と、この選択手段で選択された累積上限値と前記累積手段で累積された回数とを比較する比較手段と、この比較手段の比較結果に基づき前記複数の第１のデータ列のうち選択された第１のデータ列の使用を禁止する禁止手段とを具備している。

（作用）

たとえば暗証番号の照合不一致時に参照する累積上限値を複数登録しておき、本装置内で定められた対応関係に基づき累積上限値を選択することにより、参照する累積上限値が複数の暗証番号に対して共通に使用されなくなり、暗証番号自身のセキュリティレベルの格差を確立できる。これにより、たとえばＩＣカードシステムのセキュリティ性確立方法が多様化する。

（実施例）

以下、本発明の一実施例について図面を参照して説明する。

第２０図は本発明に係る携帯可能電子装置としてのＩＣカードを取扱う端末装置の構成例を示すものである。すなわち、この端末装置は、ＩＣカード１をカードリーダ・ライタ２を介してＣＰＵなどからなる制御部３と接続可能にするとともに、制御部３にキーボード４、ＣＲＴディスプレイ装置５、プリンタ６およびフロッピィディスク装置７を接続して構成される。

ＩＣカード１は、ユーザが保持し、たとえば商品購入などの際にユーザのみが知得している暗証番号の参照や必要データの蓄積などを行なうもので、たとえば第１８図にその機能ブロックを示す

ように、リード・ライト部１１、暗証設定・暗証照合部１２、および暗号化・復号化部１３などの基本機能を実行する部分と、これらの基本機能を管理するスーパバイザ１４とで構成されている。リード・ライト部１１は、データメモリなどに対してデータの読出し、書込み、あるいは消去を行なう機能である。暗証設定・暗証照合部１２は、ユーザが設定した暗証番号の記憶および読出禁止処理を行なうとともに、暗証番号の設定後にその暗証番号の照合を行ない、以後の処理の許可を与える機能である。暗号化・復号化部１３は、たとえば通信回線を介して制御部３から他の端末装置へデータを送信する場合の通信データの漏洩、偽造を防止するための暗号化や暗号化されたデータの復号化を行なうものであり、たとえばＤＥＳ（Data Encryption Standard）など、充分な暗号強度を有する暗号化アルゴリズムにしたがってデータ処理を行なう機能である。スーパバイザ１４は、カードリーダ・ライタ２から入力された機能コードもしくはデータの付加された機能コードを解読し、前記基本機能のうち必要な機能を選択して実行させる機能である。

これらの諸機能を発揮させるために、ＩＣカード１は、たとえば第１７図に示すように、ＣＰＵなどの制御素子（制御部）１５、データメモリ（メモリ部）１６、プログラムメモリ１７、およびカードリーダ・ライタ２との電気的接触を得るためのコンタクト部１８によって構成されており、これらのうち制御素子１５、データメモリ１６、およびプログラムメモリ１７は１つのＩＣチップ（あるいは複数のＩＣチップ）で構成されてＩＣカード本体内に埋設されている。プログラムメモリ１７は、たとえばマスクＲＯＭで構成されており、前記各基本機能を実現するサブルーチンを備えた制御素子１５の制御プログラムなどを記憶するものである。データメモリ１６は、各種データの記憶に使用され、たとえばＥＥＰＲＯＭなどの消去可能な不揮発性メモリで構成されている。

カードリーダ・ライタ２は、ＩＣカード１と制御部３との間で機能コードやデータの授受を行なうものであり、制御部３からのマクロ命令に基づいてＩＣカード１に対して１命令１応答動作を行なう機能をも有している。具体的には、たとえば第１９図に示すように、図示しないカード挿入口に挿入されたＩＣカード１を所定の位置まで搬送する搬送機構２１、所定の位置にセットされたＩＣカード１のコンタクト部１８に電気的に接触されるコンタクト部２２、全体の制御を司るＣＰＵなどからなる制御部２３、制御部２３と制御部３との間で命令データや応答データの授受を行なうための入出力インタフェイス回路２４、およびデータを記憶するデータメモリ２５などから構成されている。

前記データメモリ１６は、たとえば第３図に示すように、エリア定義テーブル１６１、暗証情報テーブル１６２、およびデータエリア１６３に大別されており、特にエリア定義テーブル１６１には、暗証情報エリア定義テーブル１６４およびトランザクションデータエリア定義テーブル１６５を含んでいる。

暗証情報エリア定義テーブル１６４は、データエリア１６３内に暗証情報エリアを定義する定義情報が格納されており、この定義情報は、たとえば第４図に示すように、エリア番号、エリア先頭アドレス、およびエリアサイズからなる一連のデータ列の集合体である。

トランザクションデータエリア定義テーブル１６５は、データエリア１６３内にトランザクションデータエリアを定義する定義情報が格納されており、この定義情報は、たとえば第５図に示すように、エリア番号、エリア先頭アドレス、エリアサイズ、およびアクセス条件情報からなる一連のデータ列の集合体である。

データエリア１６３は、暗証情報エリア定義テーブル１６４およびトランザクションデータエリア定義テーブル１６５によってエリア定義され、種々のデータが格納されるもので、その具体例を第６図に示す。

暗証情報テーブル１６２は、たとえば第７図に示すように、インデックス部、暗証番号エリアの

エリア番号部、エラーカウンタエリアのエリア番号部、エラーリミットエリアのエリア番号部、および暗証照合状態エリアのエリア番号部からなる一連のデータ列の集合体である。

インデックス部は、後述する暗証照合命令データ（第２図参照）中のインデックス指定情報と関連付けられて動作するようになっている。すなわち、暗証照合命令データ中のインデックス指定情報と同一のインデックスを捜し、見付かれば、それに対応する暗証番号などが照合の対象となるのである。

暗証番号エリアのエリア番号部は、照合対象として指定された暗証番号が格納されているデータエリア１６３内の暗証番号エリアのエリア番号である。

エラーカウンタエリアのエリア番号部は、制御素子１５内のＲＡＭ上にある第１のエラーカウンタ（第８図参照）を指定するとともに、データエリア１６３内の第２のエラーカウンタエリアのエリア番号となっている。

エラーリミットエリアのエリア番号部は、第１および第２のエラーカウンタのリミット値（累積上限値）が格納されているデータエリア１６３内のエラーリミットエリアのエリア番号である。なお、このエラーリミットエリアは１バイトエリアであり、たとえば第９図にそのフォーマットを示すように、上位４ビットで第１のエラーカウンタのリミット値を示し、下位４ビットで第２のエラーカウンタのリミット値を示す。

暗証照合状態エリアのエリア番号部は、制御素子１５内のＲＡＭ上にある照合状態ビット（第１０図参照）のどのビットを照合状態フラグとするかを識別する情報が格納されているデータエリア１６３内の暗証照合状態エリアのエリア番号である。

たとえばインデックス「３１」を指定すると、これに対応する暗証番号エリアのエリア番号は第７図により「０１」である。これを第４図に示す暗証情報エリア定義テーブル１６４から検索し、対応するエリア先頭アドレス「ＴＡ。」およびエリアサイズ「１０バイト」より、第６図に示すデータエリア１６３を参照し、暗証番号「１１１１１１１１」を得る。ここで、暗証番号エリアは、１バイトの暗証番号のバイト数を示すレングス部と可変長の暗証番号部からなっている。レングス部が“ＦＦ”Ｈｅｘのときは暗証番号が格納されていないと認識する。

次に、対応するエラーカウンタエリアのエリア番号は、第７図により「１１」となっているので、同様にしてエリア先頭アドレスＴＡ。およびエリアサイズ「１バイト」より、第６図に示すデータエリア１６３を参照し、第２のエラーカウンタの値「００」を得る。

同様な方法で、インデックス「３１」によって指定された暗証番号は８バイトデータで「１１１１１１１１」という値、また第２のエラーカウンタの値は「００」、エラーリミット値は第１のエラーカウンタとして「３」、第２のエラーカウンタとして「５」であり、照合状態ビットは第１０図の０ビット目に対応することをＩＣカード１の制御素子１５が認識するようになっている。

次に、このような構成において動作を説明する。まず、カードリーダ・ライタ２は、第１１図に示すフローチャートにしたがって動作する。すなわち、定常状態においては、制御部３からの命令データ待ち状態となっている。この状態において、制御部３から命令データが入力されると、制御部２３は、ＩＣカード１が実行中であるか否かを判断し、実行中である場合には多重命令データエラーを意味する応答データを制御部３に出力し、命令データ待ち状態に戻る。ＩＣカード１が実行中でない場合には、制御部２３は、ＩＣカード１に命令データを出力し、ＩＣカード１からの応答データ待ち状態となる。ＩＣカード１からの応答データがあると、制御部２３は、命令がマクロ命令である場合には再びＩＣカード１に命令データを出力し、そうでない場合には制御部３に応答データを出力し、命令データ待ち状態に戻る。

なお、カードリーダ・ライタ２からＩＣカード

1に出力される命令データは、たとえば第12図に示すようなフォーマットであり、同図（a）に示すように機能コードのみの形態、または同図（b）に示すように機能コードにデータを付加した形態がある。

ICカード1は、第13図に示すフローチャートにしたがって動作する。すなわち、定常状態においては、カードリーダ・ライタ2からの命令データ待ち状態となっている。この状態において、カードリーダ・ライタ2から命令データが入力されると、制御素子15は、その命令データにしたがって基本機能を実行し、カードリーダ・ライタ2にその処理結果を示す応答データを出力し、命令データ待ち状態に戻る。

この場合の応答データは、たとえば第14図に示すようなフォーマットであり、処理結果を示す情報に入力された命令データに含まれた機能コードを付加し、カードリーダ・ライタ2との間のシーケンスが乱れた場合の防護措置を講じておく。

次に、暗証番号の照合動作について第1図に示すフローチャートを参照して説明する。命令データが入力されると、制御素子15は、その命令データが例えば第2図に示すようなフォーマットを持つ暗証照合命令データであるか否か判断する。ここに、暗証照合命令データは、暗証照合機能コード、インデックス指定情報、および暗証番号情報（暗証番号レングスと暗証番号とからなる）によって構成されている。上記判断の結果、暗証照合命令データでなければ、制御素子15は、命令データ中の機能コードを解読し、対応する処理を実行した後、その処理結果に対する応答データを出力し、命令データ待ち状態に戻る。

上記命令データの判断の結果、暗証照合命令データであった場合、制御素子15は、命令データ中のインデックス指定情報と一致するインデックスをデータメモリ16内の暗証情報テーブル162のインデックス部から検索する。この検索の結果、見付からなければ、制御素子15は、実行不可を意味する応答データを出力し、命令データ待ち状態に戻る。上記検索の結果、見付かったならば、制御素子15は、そのインデックスに対応する暗証番号エリアを参照する。ここで、もし暗証番号エリアのレングス部が"FF" Hexとなっていれば、制御素子15は、暗証番号が格納されていないと認識し、暗証番号未設定を意味する応答データを出力し、命令データ待ち状態に戻る。

もし、暗証番号エリアのレングス部が"FF" Hex以外であれば、制御素子15は、暗証番号が格納されているものと認識し、次に対応する第2のエラーカウンタの値およびそのリミット値を読出し、両者の比較照合を行なう。この比較照合の結果、もしリミット値が第2のエラーカウンタの値よりも大きければ、制御素子15は、暗証番号の照合処理を行なう。上記比較照合の結果、もしリミット値が第2のエラーカウンタの値よりも大きくなければ、制御素子15は、インデックスに対応する暗証照合状態エリアを参照し、そのエリアの内容を読出すことにより、対応する照合状態ビットを「0」にし、暗証番号使用不可を意味する応答データを出力し、命令データ待ち状態に戻る。

さて、暗証番号の照合処理では、入力された命令データ中の暗証番号情報と指定された暗証番号とを比較照合する。この比較照合の結果、もし両者が一致していれば、制御素子15は、第1および第2のエラーカウンタを「00」とした後、インデックスに対応する暗証照合状態エリアを参照し、そのエリアの内容を読出すことにより、対応する照合状態ビットを「1」にし、照合完了を意味する応答データを出力し、命令データ待ち状態に戻る。

上記暗証番号の比較照合の結果、もし両者が一致していなければ、制御素子15は、インデックスに対応するエラーリミットエリアを参照し、そのエリアの内容を読出すことにより、下位4ビットの値（第2のエラーカウンタのリミット値）が「0」となっているか否かを判断する。この判断の結果、もし「0」となっていれば、制御素子15は、インデックスに対応する暗証照合状態エ

リアを参照し、そのエリアの内容を読出すことにより、対応する照合状態ビットを「０」にし、暗証番号不一致を意味する応答データを出力し、命令データ待ち状態に戻る。

上記エラーリミットエリアの下位４ビットの値の判断の結果、もし「０」となっていなければ、制御素子１５は、エラーリミットエリアの上位４ビットの値（第１のエラーカウンタのリミット値）と第１のエラーカウンタの値とを比較照合する。この比較照合の結果、もし前者が後者よりも大きければ、制御素子１５は、対応する第１のエラーカウンタの値を１つ増加する。そして、制御素子１５は、インデックスに対応する暗証照合状態エリアを参照し、そのエリアの内容を読出すことにより、対応する照合状態ビットを「０」にし、暗証番号不一致を意味する応答データを出力し、命令データ待ち状態に戻る。

上記エラーリミットエリアの上位４ビットの値と第１のエラーカウンタの値との比較照合の結果、もし前者が後者よりも大きくなければ、制御素子１５は、インデックスに対応する第２のエラーカウンタエリアを参照し、そのエリアの内容を読出すことにより、第２のエラーカウンタの値と対応するリミット値（下位４ビットの値）とを比較照合する。この比較照合の結果、もし前者よりも後者の方が大きければ、制御素子１５は、対応する第２のエラーカウンタの値を１つ増加する。そして、制御素子１５は、インデックスに対応する暗証照合状態エリアを参照し、そのエリアの内容を読出すことにより、対応する照合状態ビットを「０」にし、暗証番号不一致を意味する応答データを出力し、命令データ待ち状態に戻る。

上記第２のエラーカウンタの値と対応するリミット値との比較照合の結果、もし前者よりも後者の方が大きくなければ、制御素子１５は、インデックスに対応する暗証照合状態エリアを参照し、そのエリアの内容を読出すことにより、対応する照合状態ビットを「０」にし、暗証番号使用不可を意味する応答データを出力し、命令データ待ち状態に戻る。

なお、第７図で示すように、エラーカウンタエリアのエリア番号「１２」および「１３」は、インデックス「３２」と「３３」および「３４」と「３５」にそれぞれ対応している。これは、照合命令対象としてインデックス「３２」に対応する暗証番号としても、また「３３」に対応する暗証番号としても同一のエラーカウンタを使用することになる。また、インデックス「３４」と「３５」も同様な関係にある。さらに、特にインデックス「３４」と「３５」については、エラーリミット値も共有（エリア番号として「２４」を共通に使用）している。これにより、たとえばインデックス「３４」を使用した暗証番号の照合において、第２のエラーカウンタがリミット値に達してしまうと、同時にインデックス「３５」を使用した暗証番号の照合も行なえなくなる。

また、インデックス「３２」と「３３」に対応する暗証照合状態エリアのエリア番号も同一の「４２」というエリア番号を示している。したがって、どちらを用いて照合を行なっても照合状態フラグは第１０図において１ビット目が「１」となる。

次に、トランザクションデータの書込み動作について第１５図に示すフローチャートを参照して説明する。先の第１図において、入力された命令データが暗証照合命令データでなければ、制御素子１５は、次に入力された命令データが第１６図に示すようなフォーマットを持つトランザクションデータ書込み命令データか否かを判断する。ここに、トランザクションデータ書込み命令データは、トランザクションデータ書込み機能コード、エリア指定情報、および書込みデータによって構成されている。上記判断の結果、トランザクションデータ書込み命令データでなければ、制御素子１５は、命令データ中の機能コードを解読し、対応する処理を実行した後、その処理結果に対する応答データを出力し、命令データ待ち状態に戻る。

上記命令データの判断の結果、トランザクションデータ書込み命令データであった場合、制御素子１５は、命令データ中のエリア指定情報と一致

するエリア番号をデータメモリ１６内のトランザクションデータエリア定義テーブル１６５から検索する。この検索の結果、見付からなければ、制御素子１５は、エリア未定義を意味する応答データを出力し、命令データ待ち状態に戻る。

上記エリア番号の検索の結果、見付かったならば、制御素子１５は、そのエリア番号に対応するアクセス条件情報を参照し、そのアクセス条件情報の示す照合状態ビットが「１」になっているか否かを判断する。この判断の結果、もし「０」であれば、制御素子１５は、アクセス不可を意味する応答データを出力し、命令データ待ち状態に戻る。上記判断の結果、もし「１」であれば、制御素子１５は、トランザクションデータの書込み処理を行ない、その処理結果に対応する応答データを出力し、命令データ待ち状態に戻る。

たとえば、第５図を参照すると、エリア番号「８０」に対してはアクセス条件情報は「０４」となっているので、照合状態ビットの２ビット目が「１」となっていれば、トランザクションデータの書込みは可能である。したがって、インデックス「３４」を用いた暗証番号の照合が正常に終了すれば、データエリア１６３内のエリア「８０」にデータ書込みが行なえることになる。また、エリア番号「８１」は照合状態ビットの１ビット目が関係しているため、インデックス「３２」または「３３」を用いた暗証番号の照合が正常に終了すれば、データエリア１６３内のエリア「８１」にデータ書込みが行なえることになる。

このように、暗証番号の照合不一致時に参照する累積上限値（リミット値）を複数登録しておき、本ＩＣカード内で定められた対応関係に基づき累積上限値を選択することにより、参照する累積上限値が複数の暗証番号に対して共通に使用されなくなり、暗証番号自身のセキュリティレベルの格差を確立できる。これにより、ＩＣカードシステムのセキュリティ性確立方法が多様化する。

なお、前記実施例では、携帯可能電子装置としてＩＣカードを例示したが、本発明はカード状のものに限定されるものではなく、たとえばブロック状あるいは棒状のものでもよい。また、携帯可能電子装置のハード構成も、その要旨を逸脱しない範囲で種々変形可能である。

【発明の効果】

以上詳述したように本発明によれば、暗証番号の照合不一致時に参照する累積上限値が複数の暗証番号に対して共通に使用されなくなり、暗証番号自身のセキュリティレベルの格差を確立できる携帯可能電子装置を提供できる。

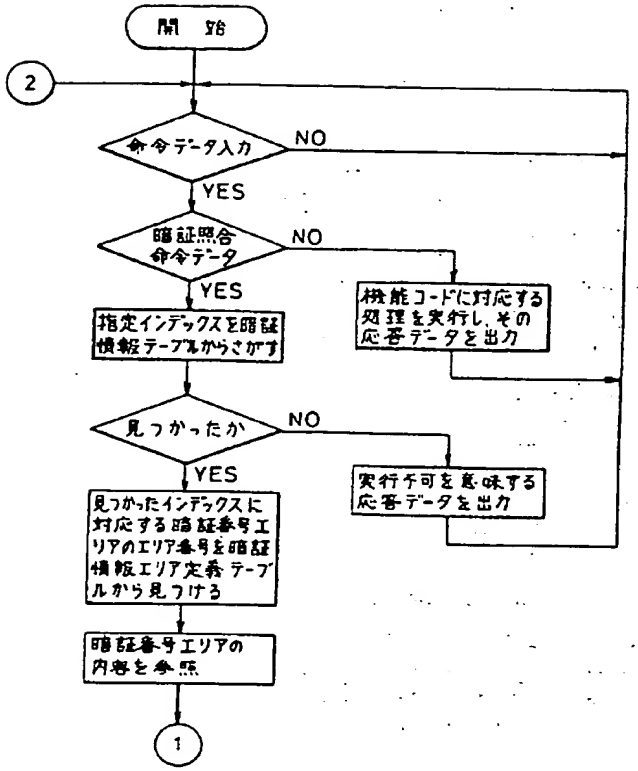
４．図面の簡単な説明

図は本発明の一実施例を説明するためのもので、第１図は暗証番号の照合動作を説明するフローチャート、第２図は暗証照合命令データのフォーマット例を示す図、第３図はデータメモリのフォーマット例を示す図、第４図は暗証情報エリア定義テーブルの具体例を示す図、第５図はトランザクションデータエリア定義テーブルの具体例を示す図、第６図はデータエリア内の格納データの具体例を示す図、第７図は暗証情報テーブルの具体例を示す図、第８図は第１のエラーカウンタエリアを示す図、第９図はエラーカウンタエリアに格納されているリミット値のフォーマット例を示す図、第１０図は照合状態ビットのフォーマット例を示す図、第１１図はカードリーダ・ライタの動作を説明するフローチャート、第１２図はＩＣカードに入力される命令データのフォーマット例を示す図、第１３図はＩＣカードの動作を説明するフローチャート、第１４図はＩＣカードから出力される一般的な応答データのフォーマット例を示す図、第１５図はトランザクションデータの書込み動作を説明するフローチャート、第１６図はトランザクションデータ書込み命令データのフォーマット例を示す図、第１７図はＩＣカードの構成を示すブロック図、第１８図はＩＣカードの機能ブロックを示す図、第１９図はカードリーダ・ライタの構成を示すブロック図、第２０図は端末装置の構成を示すブロック図である。

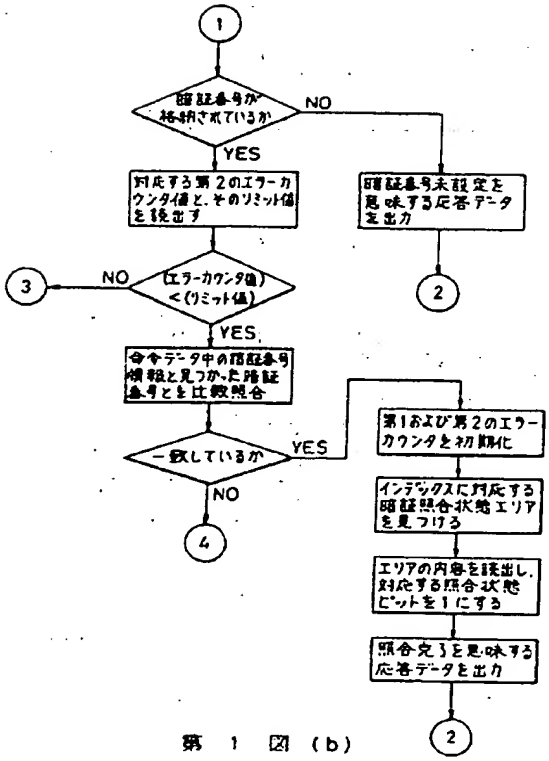
１…ＩＣカード（携帯可能電子装置）、１５…制御素子（制御部）、１６…データメモリ（メモリ部）、１７…プログラムメモリ、１６１…エリ

ア定義テーブル、１６２…暗証情報テーブル、１６３…データエリア、１６４…暗証情報エリア定義テーブル、１６５…トランザクションデータエリア定義テーブル。

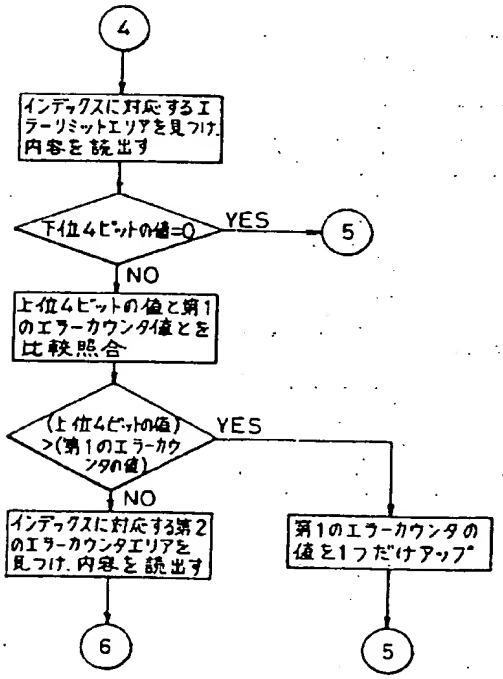
出願人代理人　弁理士　鈴江武彦



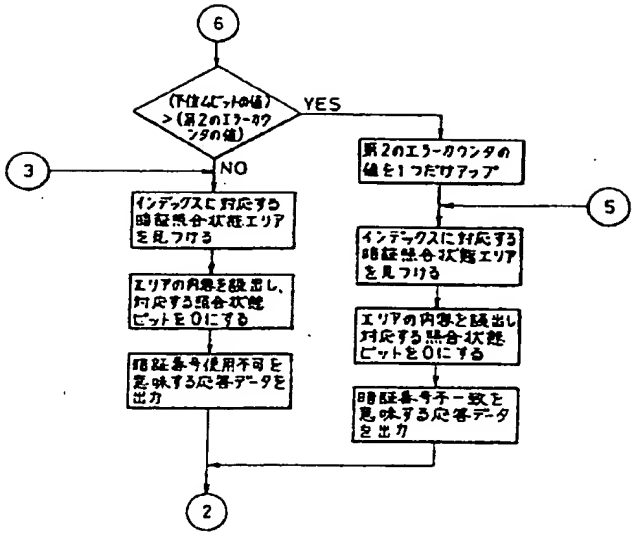
第　1　図　(a)



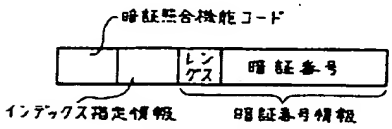
第　1　図　(b)



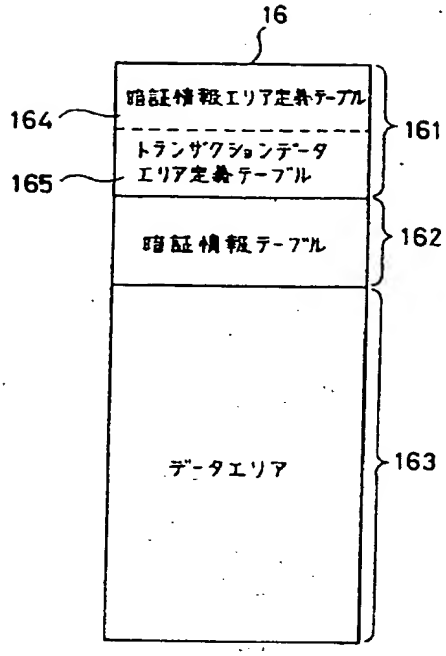
第　1　図　(c)



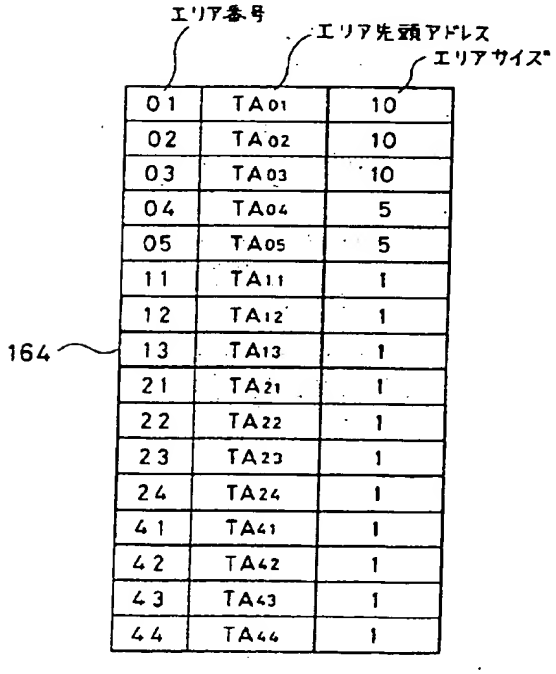
第 1 図 (d)



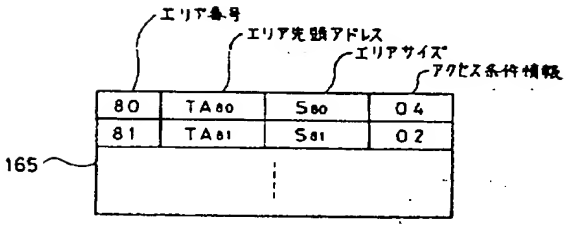
第 2 図



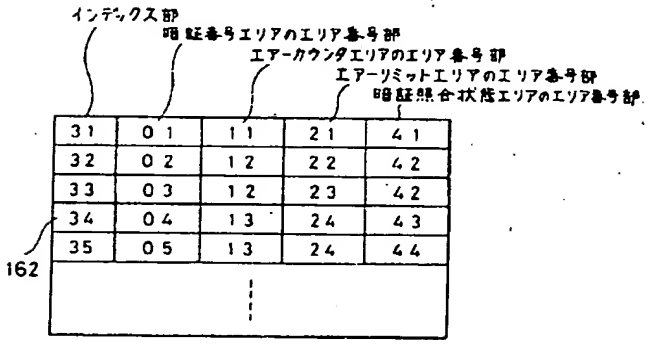
第 3 図



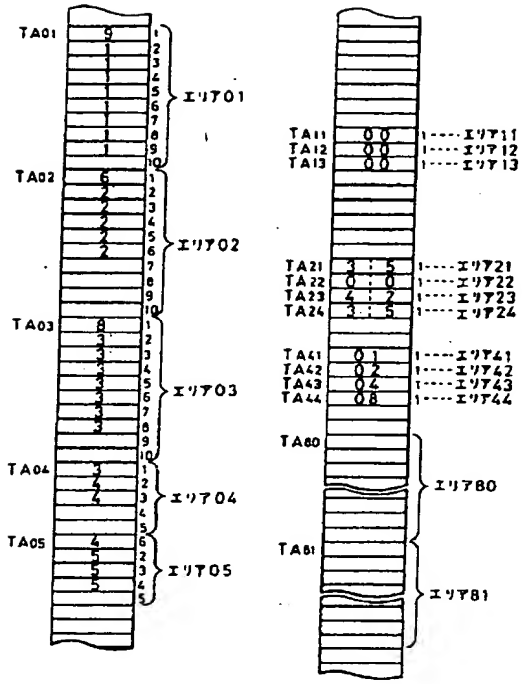
第 4 図



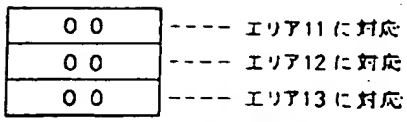
第 5 図



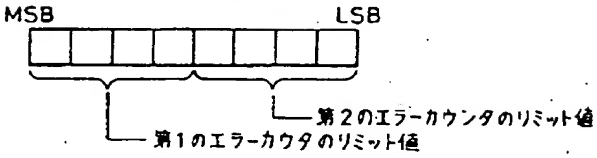
第 7 図



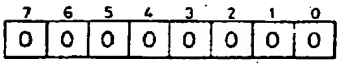
第 6 図



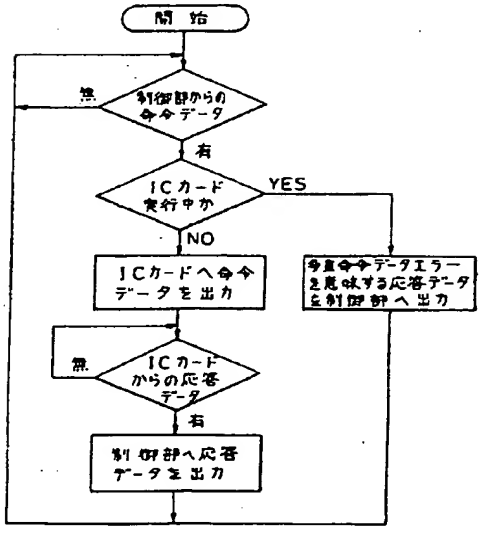
第 8 図



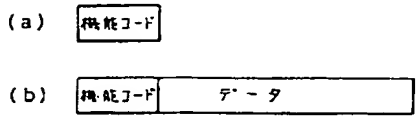
第 9 図



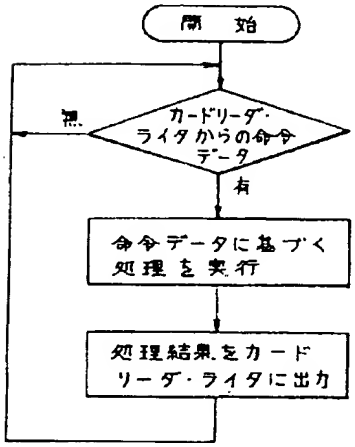
第 10 図



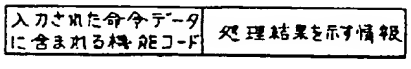
第 11 図



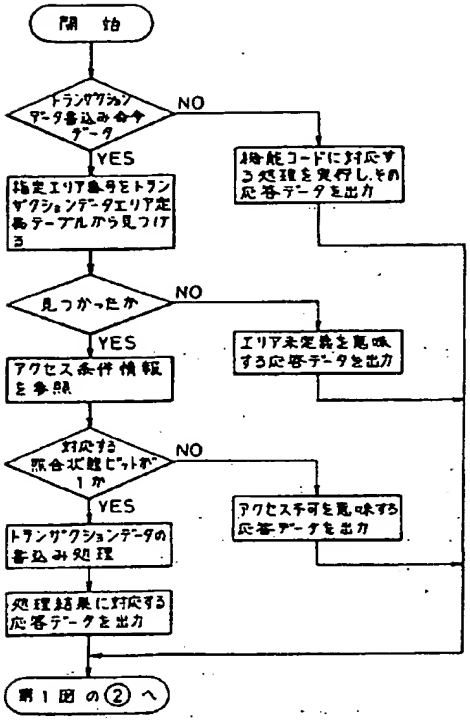
第 12 図



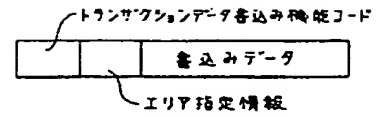
第 13 図



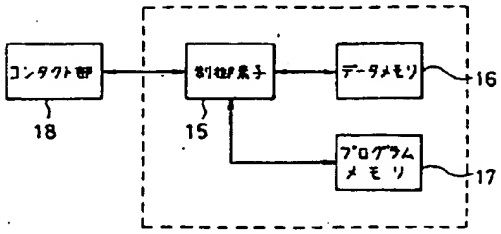
第 14 図



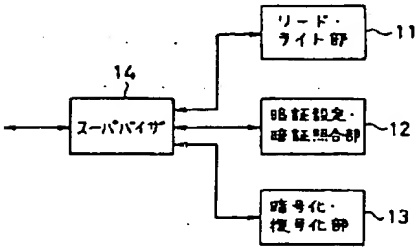
第 15 図



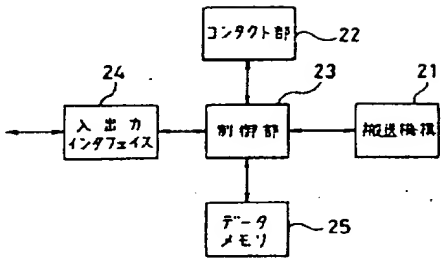
第 16 図



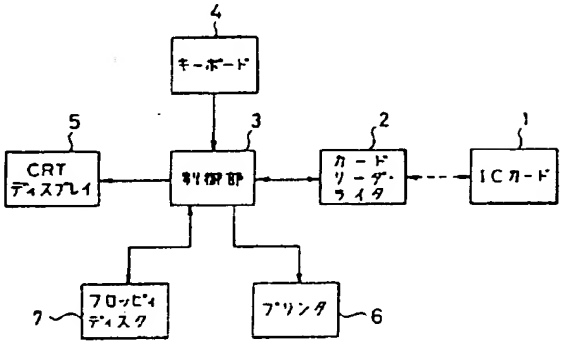
第 17 図



第 18 図



第 19 図



第 20 図